$E_A(M)$ sent to him. If user A wants to send a response to user B, user A enciphers the message using user B's encryption key E_B, also available in the public file. Therefore no transactions between users A and B, such as exchange of secret keys, are required to initiate private communication. The only "setup" required is that each user who wishes to receive private communication must place his enciphering key E in the public file.

The public key approach of Diffie and Hellman is also useful in principle to provide signed digital messages that are both message-dependent and signer-dependent. The recipient of a "signed" message not only knows the message substance, but also can provide that the message originated from the identified sender. A signed message precludes the possibility that a recipient could modify the received message by changing a few characters or that the recipient could attach the received signature to any message whatsoever. This is a particular problem for digital messages inasmuch as electronic "cutting and pasting" of sequences of characters are generally undetectable in the final product.

In order to implement signatures on messages transferred between two users, e.g. user A and user B, in accordance with the Diffie and Hellman system, each user has encoding keys E_A and E_B, respectively, on a public file and decoding keys D_A and D_B, respectively, privately held. Each user's encoding and decoding keys must effect permutations of the same message space S, so that the following relation s hold:

$$D_A(E_A(M)) = M$$

$$E_A(D_A(M)) = M$$

$$D_B(E_B(M)) = M$$

$$E_B(D_B(M)) = M$$

for any message M.

When user A wants to send user B a "signed" document M, user A first uses his own decryption key D_A to transform M into a signed message word $M_s = D_A(M)$. User A then uses user B's encryption key E_B (from the public file) to generate a signed ciphertext word $C_s = E_B(M_s) = E_B(D_A(M))$, which is sent to user B. User B initially uses his secret decryption key D_B to reduce the signed ciphertext C_s to a signed message word in accordance with $D_B(C_s) = D_B(E_B(M_s)) = M_s$. Now using user A's encoding key E_A (available from the public file), user B decodes the signed message word in accordance with $E_A(M_s) = E_A) = M$.

User A cannot deny having sent user B this message, since no one but A could have created $M_s = D_A(M)$, provided that D_A is not computable from E_A. Furthermore, user B can show that the public key E_A is necessary to extract the message M so that user B has "proof" that user A has signed the document. User B cannot modify M to a different version M', since then user B would have to create the corresponding signature $D_A(M')$ as well. Therefore user B must have received a document "signed" by A, which he can "prove" that A sent, but which B cannot modify in any detail.

While the public-key cryptosystem principles as described above, and their potential use as a means of implementing digital "signatures", are known in the prior art, there are no practical implementations which are known, either with or without signature.

Accordingly, it is an object of this invention to provide a system and method for implementing a private communications system.

It is another object to provide a system and method for establishing a private communications system for transmission of signed messages.

It is still another object to provide a system and method for implementing a public key cryptographic communications system.

It is a further object to provide a system and method for encoding and decoding digital data.

SUMMARY OF THE INVENTION

Briefly, the present invention includes at least one encoding device, at least one decoding device, and a communication channel, where the encoding and decoding devices are coupled to the channel. The encoding device is responsive to an applied message-to-be-transmitted M and an encoding key to provide a ciphertext word C for transmission to a particular decoding device. The encoding key E is a pair of positive integers e and n which are related to the particular decoding device. The message M is a number representative of a message-to-be-transmitted and wherein

$$0 \leqq M \leqq n - 1$$

where n is a composite number of the form

$$n = p \cdot q$$

ps where p and q are prime numbers.

For messages represented by numbers outside the range 0 to $n-1$, a conventional blocking means is utilized to break the message into message block words before encoding, where each block word is representative of a number within the specified range. Following subsequent decoding, the recovered block words may be transformed back to the original message.

The presently described encoding device can distinctly encode each of the n possible messages. In alternative but equivalent embodiments, the numbers representative of the possible messages-to-be-transmitted need not be integers in the range 0 to $n-1$, but could be integers selected from each residue class modulo n. For example, where $n=3$, the numbers representative of the set of messages-to-be-transmitted might include $0(\equiv 0 \bmod 3)$, $10(\equiv 1 \bmod 3)$, and $8(\equiv 2 \bmod 3)$. Accordingly, the range limitations for n expressed hereafter in this application are appropriate for the numbers in the modulo residue classes within the respective ranges, but it will be understood that numbers outside the range but selected from the appropriate residue classes are considered to be equivalent to those within the specified range and are intended to be embraced by the claims.

The transformation provided by the encoding device is described by the relation

$$C \equiv M^e \pmod{n}$$

where e is a number relatively prime to $(p-1)\cdot(q-1)$.

The particular decoding device is also coupled to the channel and is adapted to receive the ciphertext C from the channel. The decoding device is responsive to the received ciphertext word C and a decoding key to transform that ciphertext to a received message word M'. The decoding key D is a pair of positive integers d and n. M' is a number representative of a deciphered